EL PAPEL DE LA INSPECCIÓN DE TRABAJO COMO GARANTE DE LOS DERECHOS DIGITALES DE LOS TRABAJADORES[*]

Aránzazu Roldán Martínez[**]
Universidad de Alcalá

SUMARIO: 1. Introducción. –2. Los derechos digitales de los trabajadores. Especial referencia a los bienes jurídicos protegidos; 2.1. El derecho a la intimidad y uso de los dispositivos digitales en el ámbito laboral; 2.2. El derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo; 2.3. El derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral; 2.4. El derecho a la desconexión digital en el ámbito laboral. –3. Procedimiento sancionador. –4. La posible concurrencia de competencias entre la Inspección de Trabajo y la AEPD.

RESUMEN

La Inspección de Trabajo y Seguridad Social es un servicio público al que corresponde ejercer la vigilancia del cumplimiento de las normas del orden social y exigir las responsabilidades pertinentes. En buena lógica, es competente para sancionar los incumplimientos de los derechos digitales de los trabajadores regulados en el artículo 20 bis) ET, dada su clara naturaleza laboral, aunque la LISOS no contiene unos tipos infractores específicos. Este trabajo estudia los derechos digitales de los trabajadores, haciendo especial hincapié en los bienes jurídicos protegidos, tras lo cual analiza en qué preceptos de la LISOS podría basar la Inspección de Trabajo su actuación sancionadora. Por último, y dado que los términos de su ejercicio se fijan en la Ley Orgá-

[*] Recibido el 10 de octubre de 2023. Aprobado el 26 de octubre de 2023.
[**] Profesora Ayudante Doctora de Derecho del Trabajo y de la Seguridad Social.

nica 3/2018, de protección de datos personales y garantía de los derechos digitales, se identificarán posibles problemas de concurrencia con las competencias de la AEPD, cuya solución podría exigir la aplicación del principio non bis in idem.

ABSTRACT

The Labor and Social Security Inspection is a public service responsible for monitoring compliance with the rules of social order and demanding the relevant responsibilities. Logically, it is competent to sanction non-compliance with the digital rights of workers regulated in article 20 bis) ET, given its clear labor nature, although the LISOS does not contain specific types of infringements. This work studies the digital rights of workers, placing special emphasis on the protected legal assets, after which it analyzes which precepts of the LISOS the Labor Inspection could base its sanctioning actions on. Finally, and given that the terms of its exercise are set out in Organic Law 3/2018, on the protection of personal data and guarantee of digital rights, possible problems of concurrence with the powers of the AEPD will be identified, the solution of which could require the application of the non bis in idem principle.

Palabras clave: Derechos digitales en el ámbito laboral, videovigilancia, audiovigilancia, geolocalización, desconexión digital, derecho a la intimidad, derecho a la protección de datos, principio *non bis in idem.*

Key words: Digital rights in the workplace, video surveillance, audio surveillance, geolocation, digital disconnection, right to privacy, right to data protection, *non bis in idem* principle.

1. INTRODUCCIÓN

Nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso en el artículo 18.4 que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». A través de este derecho se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención [STC 94/1998, de 4 de mayo (FJ 4)]. Como aclaró la STC 292/2000, de 30 de noviembre, se trata de un derecho autónomo e independiente del derecho a la intimidad, frente al que presenta dos peculiaridades. La primera reside en su objeto que no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, pues para ello está

la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo. Una segunda peculiaridad radica en su contenido, ya que a diferencia del derecho a la intimidad, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos (derechos ARCO). En definitiva, el poder de disposición sobre los datos personales.

Los constituyentes de 1978 intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. En el apartado IV del Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales —en adelante LOPDyGDD—, que se propone como primer objetivo adaptar el Reglamento general de protección de datos —en adelante, RGPD—[1], el legislador muestra su deseo de que una futura reforma de la Constitución incluyera entre sus prioridades la actualización de la norma fundamental a la era digital «y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea». De esta forma, el artículo 1 de la LOPDyGDD añade un segundo objetivo a la norma: «b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución». La concreción de este nuevo elenco de derechos se abordó en el Título X. Cuatro de ellos se desarrollan específicamente en el ámbito laboral y se regulan en los siguientes preceptos:

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Artículo 88. Derecho a la desconexión digital en el ámbito laboral.
- Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
- Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

El propio título de los artículos habla expresamente del «derecho a la intimidad», con la excepción del artículo 88, que según la DF 1.ª tiene carácter ordinario. Sin embargo, el Preámbulo de la Ley Orgánica sí lo vincula a este derecho fundamental cuando quiere destacar el lugar relevante que ocupa en el nuevo elenco de derechos «el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral». Se trata de derechos con un marcado carácter laboral como lo prueba el hecho de que la DF 13.ª añadiera un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre —en adelante, ET—, con el siguiente contenido: «Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.» Sistemáticamente, el artículo 20 bis) se ha situado a continuación del artículo 20, que regula el poder de dirección y control del empresario y no dentro del artículo 4.2 que regula los derechos básicos de los trabajadores con relevancia constitucional, lo que ha llevado a Altés Tárrega[2] a afirmar que no sería aplicable la infracción específica del artículo 4 recogida en el artículo 7.10 Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social —en adelante, LISOS—. Sobre ello volveremos más adelante. El nuevo precepto regula dos categorías de derechos[3]:

a) Tres derechos de intimidad: derechos que tratan de proteger el derecho a la intimidad del trabajador frente al poder de control del empleador sobre el desarrollo de la actividad laboral, llevado a cabo mediante dispositivos digitales, videovigilancia, audiovigilancia y geolocalización[4]. En este sentido, el artículo 20 bis) desarrolla el derecho a la intimidad de los trabajadores del artículo 4.1.e) ET, en el entorno digital.

---

[2] ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías de *lege data», Labos,* vol. 1, núm. 2, p. 66.

[3] QUÍLEZ MORENO, J. M., «La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores», *Revista Española de Derecho del Trabajo* núm.217, 2019, p. 4.

[4] Critica QUÍLEZ MORENO, J. M., («La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores», *op. cit.*, p. 6), la inclusión de estos derechos digitales en el ámbito laboral

b) El derecho a la desconexión digital.

El contenido concreto de estos derechos digitales se desarrolla con mayor o menor fortuna en el texto de la ley orgánica. Respecto de los tres derechos de intimidad, lo que ha hecho el legislador es incorporar los criterios utilizados por la jurisprudencia del TEDH, al interpretar el artículo 8 del Convenio para la protección de los derechos humanos y libertades fundamentales, al objeto de garantizar la protección de los derechos digitales de la persona trabajadora, pero también la jurisprudencia de la Sala cuarta del Tribunal Supremo y la de nuestro Tribunal Constitucional.

Partiendo de la base de que la Inspección de Trabajo es competente para vigilar el cumplimiento de las normas de orden social y exigir las responsabilidades pertinentes (artículo 1.2 de la Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social —en adelante, LOITSS—), sería competente para conocer de los incumplimientos del artículo 20 bis) ET. En este sentido, está llamada a desempeñar un papel esencial sancionando las conductas más graves y requiriendo a los empresarios para que cumplan con sus obligaciones legales y convencionales[5]. No tenemos, sin embargo, la posibilidad de conocer el resultado de dichas actuaciones, ya que, a diferencia de las resoluciones de la AEPD, las actas de infracción de la ITSS no son públicas. La autora de este trabajo presentó a través del portal de Transparencia solicitud de información al Ministerio de Trabajo y Economía Social, sobre «las sanciones que la ITSS ha impuesto desde el año 2019, por infracción de los derechos digitales del trabajador, regulados en los arts. 87 a 90 de la LO 3/2018». Mediante Resolución Exp.: 001-00077777, la Directora del Organismo Estatal Inspección de Trabajo denegó dicha información por la complejidad que supone reunir los datos solicitados. Tras recordar que los derechos digitales son los regulados en los artículos 87 a 90 LOPDyGDD, explica que «en el Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, no se tipifican como infracciones específicas las vulneraciones de estos derechos y que, por tanto, su transgresión debe tipificarse en alguno de los preceptos regulados en la citada norma. Estos preceptos, como sería el caso del artículo 8.11 (actos del empresario que fueren contrarios al respeto de la intimidad y conside-

---

en una Ley orgánica de protección de datos y junto a otros derechos con los que no guarda ninguna relación: «El único nexo en común que fuerza el legislador, fijando el herrete en el extremo del cabo para evitar que éste se deshilache es, precisamente, que los derechos y libertades de la Constitución son plenamente aplicables en Internet, de tal modo que, pudiendo afectar las nuevas tecnologías digitales a derechos consagrados constitucionalmente, en especial a la intimidad reconocida en el artículo 18.4 de nuestra Constitución, su encaje de regulación era esta nueva Ley Orgánica de Protección de Datos, lo que, como digo, me parece un tanto forzado, pero no es este el foro adecuado para debatir estos extremos.»

[5] Por ejemplo, en la resolución de la ITSS de 7 de marzo de 2023 (OS 11/0000680/23) en contestación a la denuncia presentada por Alternativa sindical se requiere a la empresa para que cumpla las disposiciones del convenio colectivo relativas al derecho de desconexión digital. Fuente: Alternativa Sindical. Disponible en: https://alternativasindical.es/la-inspeccion-de-trabajo-de-cadiz-requiere-a-new-man-security-s-l-a-que-cumpla-con-lo-requerido/ (última consulta 12 de octubre de 2022).

ración debida a la dignidad de los trabajadores) resultarían aplicables a estos supuestos y a muchos otros más sin que sea posible identificar el supuesto sin analizar cada expediente. Por tanto, no es posible extraer la información solicitada sin realizar un análisis manual de los expedientes en los que se han detectado infracciones de este tipo y realizar una lectura de cada documento para poder identificar las infracciones que se derivan del incumplimiento de los preceptos solicitados»[6].

En este trabajo analizaremos en qué preceptos de la LISOS podría incluirse cada una de las vulneraciones de estos derechos. Para ello, como paso previo, analizaremos la naturaleza de estos derechos y los bienes jurídicos protegidos. A continuación, debemos preguntarnos si, tras la entrada en vigor de la ley orgánica, la competencia sancionadora corresponde exclusivamente a la ITSS o si se produce una concurrencia con la AEPD. No hay que olvidar que la AEPD con anterioridad a la entrada en vigor de la LOPDyGDD venía sancionando conductas relacionadas con la vulneración de estos derechos, principalmente en materia de videovigilancia y geolocalización. Esta actuación, tras la aprobación del RGPD, parece haberse incrementado. Como advierte Mercader Uguina, la actuación de la AEPD «muestra un incremento de las Resoluciones que tienen como objeto aspectos diversos de lo laboral». La razón puede encontrarse en que el derecho de protección de datos «se está comiendo» el derecho a la intimidad[7], entre otros motivos, porque en la Unión europea «la protección de datos lentamente empieza a ocupar espacios de la privacidad imponiendo sus principios de actuación mucho más exigentes y rigurosos que los que habían servido hasta ahora para limitar el derecho a la intimidad»[8]. En segundo lugar, el artículo 8 del Convenio europeo de derechos humanos (CEDH), cuya vulneración se alega ante el TEDH como fundamentación de demandas sobre extralimitación del poder de control del empresario por medios tecnológicos (vigilancia de correos electrónicos, videovigilancia y geolocalización), regula el derecho de toda persona al respeto a su vida privada y familiar sin diferenciar entre el derecho a la intimidad, el derecho a la propia imagen y el derecho a la protección de datos, aglutinando a todos en «un espacio más amplio, cual es el derecho a la privacidad»[9].

---

[6] La única forma de conocer las sanciones es a través de la información que proporcionan los sindicatos o de las sentencias que conocen de la impugnación de las resoluciones recaídas en los procedimientos sancionadores. No tenemos conocimiento de ninguna sentencia hasta la fecha.

[7] MERCADER UGUINA, J. y GARCÍA PERROTE ESCARTÍN, I., «La protección de datos se come a la intimidad: La doctrina de la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017», *Revista de Información Laboral,* 2017, núm. 10, pp. 7-12.

[8] *Vid*., por ejemplo, la STEDH de 13 de diciembre de 2022 —caso Florindo de Almeida Vasconcelos Gramaxo contra Portugal— sobre geolocalización.

[9] GONZÁLEZ RODRÍGUEZ, R., «Los derechos fundamentales como límite difuso al control tecnológico en el ámbito laboral: luces y sombras de la primera regulación específica sobre la materia», *Revista de Trabajo y Seguridad Social,* CEF, 2021, núm. 463, pág. 69.

2. LOS DERECHOS DIGITALES DE LOS TRABAJADORES. ESPECIAL REFERENCIA A LOS BIENES JURÍDICOS PROTEGIDOS

2.1. El derecho a la intimidad y uso de los dispositivos digitales en el ámbito laboral

Empezando por los derechos de intimidad, en el artículo 87 se regula el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. En realidad, el precepto no se refiere a todos los dispositivos digitales con independencia de quién sea su propietario, sino sólo a los profesionales, esto es los «dispositivos digitales puestos a su disposición por su empleador». El empleador podrá acceder a los contenidos derivados del uso de dichos medios únicamente en dos supuestos «a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos». Respecto del derecho de los trabajadores a utilizar los dispositivos digitales de la empresa para fines privados, se dispone que los empleadores «deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente». La fijación de estos criterios por el empresario no se sitúa en el ámbito de la responsabilidad social corporativa sino que es un auténtico deber exigible jurídicamente[10], aunque el legislador no haya previsto ninguna sanción en caso de incumplimiento en la LISOS. Tales criterios no se pueden elaborar de forma unilateral por el empresario, sino que tiene que contar con la participación de los representantes de los trabajadores, lo que se traduce en un deber de consulta que se añadiría a los previstos en el artículo 64 ET [11]. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. «Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.» Este deber de información individual concurre con el deber de información y consulta de los representantes legales de los trabajadores. En todo caso, la medida de control adoptada debe ser conforme con el parámetro de proporcionalidad necesidad e idoneidad (PIN de constitucionalidad).

---

[10] De esta opinión es BAZ RODRÍGUEZ, J., «Protección de datos y garantía de los derechos digitales laborales en el nuevo marco», *Ars Iuris Salmanticensis*, 2019, volumen 7, p. 148. También STSJ Madrid de 30 de junio de 2021 (Rec. 428/2021).

[11] SAN de 22 de julio de 2022 (Rec 178/2022). De la misma opinión es LÓPEZ AHUMADA, J. E., «Estándares de protección de la intimidad en el ámbito laboral y desarrollo del deber de información empresarial en materia de protección de datos», AA.VV. (López Ahumada, J. E., dir; Gamarra Vílchez, L. y Varela Bohórquez, F., coords.), *La gobernanza de los derechos digitales de las personas trabajadoras,* Editorial Cinca, 2023, p. 149.

Si bien del tenor literal del precepto podría interpretarse que el bien jurídico protegido es exclusivamente el derecho a la intimidad, en la medida en que el acceso a los dispositivos digitales implique un tratamiento de datos personales, premisa de la que partía el denominado Grupo de Trabajo del artículo 29[12], será exigible la aplicación de la normativa de protección de datos (RGPD y LOPDyGDD)[13]. De hecho, aunque pueda pensarse que el artículo 87 se refiera a la intimidad, «en su contenido está utilizando las garantías que se prevén para la protección de datos» y, en concreto, el deber de información, que según la STC 39/2016, de 3 de marzo (FJ 3) forma parte del contenido esencial del derecho de protección de datos, o los protocolos de uso[14]. El artículo 17.1 de la LTD es más claro cuando exige que «la utilización de los medios telemáticos y el control de la prestación laboral mediante dispositivos automáticos garantizará adecuadamente el derecho a la intimidad y a la protección de datos, en los términos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales»[15], lo cual «convierte, por remisión, en aplicables

---

[12] Hay dos documentos de la Unión europea, de gran interés para esta materia: las recomendaciones recogidas en el Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo, de 29 de mayo de 2002 (WP55), del Grupo de Trabajo del artículo 29; se complementa con el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, elaborado por el ahora denominado Grupo de Trabajo sobre protección de datos del artículo 29 —en adelante, GT 29— que ha hecho una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores.

[13] Como explica González Rodríguez, entre los derechos constitucionales protegidos si se controlan documentos de carácter personal del trabajador se puede estar afectando el derecho a la intimidad; si se controla el flujo de comunicaciones o los historiales de búsqueda, resultaría afectado el derecho de protección de datos e, incluso, podría resultar afectado el secreto de las comunicaciones si el control afecta a las comunicaciones entre el trabajador y otra personas de la empresa o extraña a ésta. GONZÁLEZ RODRÍGUEZ, R., «Los derechos fundamentales como límite difuso al control tecnológico en el ámbito laboral: luces y sombras de la primera regulación específica sobre la materia», *op. cit.*, p. 78.

[14] GONZÁLEZ RODRÍGUEZ, R., «Los derechos fundamentales como límite difuso al control tecnológico en el ámbito laboral: luces y sombras de la primera regulación específica sobre la materia», *op. cit.*, pág. 76. GOÑI SEIN, considera que «la norma garantiza al trabajador un derecho positivo a la protección de su información personal, que se traduce en el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado». *Vid,* GOÑI SEIN, J. L., «Uso de los dispositivos digitales en el ámbito laboral», *Trabajo y Derecho*, 2020, núm. 11, p. 6. En el mismo sentido, ARRÚE MENDIZÁBAL llama la atención sobre el hecho de que el artículo 87 hable sólo del derecho a la intimidad, obviando la doctrina judicial que consideraba implicados otros derechos fundamentales. En su opinión, «la vuelta a este derecho más clásico, a la intimidad, no creemos que pueda conducir a interpretaciones restrictivas en perjuicio de los derechos de los empleados porque el contenido de las garantías previsto (información previa, protocolos de uso) es el propio del derecho a la protección de datos de carácter». *Vid*, ARRÚE MENDIZÁBAL, M., «Los derechos a la intimidad, a la propia imagen y a la protección de datos de los empleados públicos vs el control por parte de la Administración», *La Administración al día, (versión digital)*, entrada del 25 de junio de 2020. LÓPEZ AHUMADA, J. E., también analiza el deber de información del empleador como un imperativo que deriva del RGPD («Estándares de protección de la intimidad en el ámbito laboral y desarrollo del deber de información empresarial en materia de protección de datos», *op. cit.*, pp. 151-156). En el mismo sentido, aplican la normativa de protección de datos RODRÍGUEZ ESCANCIANO, S., y ÁLVAREZ CUESTA, H., «La toma de decisiones automatizadas en el marco de la relación laboral: otra vuelta de tuerca al poder de dirección y vigilancia empresarial», AA.VV. (López Ahumada, J. E., dir.; Gamarra Vílchez, L. y Varela Bohórquez, F., coords.), *La gobernanza de los derechos digitales de las personas trabajadoras,* «Editorial Cinca», 2023 pp. 110-144.

[15] GARCÍA RUBIO, A., «Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa», *Labos,* Vol. 3, No. 1, pp. 21-46, doi: https://doi.org/10.20318/labos.2022.6845, p. 28.

todos sus principios: desde la simple transparencia informativa, pasando por las garantías de 'idoneidad, temporalidad, finalidad, responsabilidad proactiva, necesidad y proporcionalidad de los medios utilizados' hasta la necesidad de asegurar, a la postre, que no se utilice un determinado instrumento de control si puede haber otro menos invasivo de los derechos fundamentales del trabajador»[16]. Veremos más adelante, sin embargo, que la propia AEPD considera que el artículo 87 está excluido del ámbito de aplicación del RGPD.

2.2. El derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

En el artículo 89 se regula el derecho a la intimidad frente al uso de dispositivos de videovigilancia y audiovigilancia, esto es, la grabación de sonidos en el lugar de trabajo. Hay que precisar que la LOPDyGDD regula la videovigilancia en el artículo 22, precepto que prevé un plazo máximo para la supresión de los datos (apartado 3) y regula el dispositivo informativo que debe colocarse, para cumplir con el artículo 12 RGPD, «en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información» (apartado 4). El apartado 8 del artículo 22 establece que «el tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica». En este sentido el artículo 89 es una norma especial que se ciñe al ámbito exclusivamente laboral, permitiendo a los empleadores «tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo».

Nuevamente se recoge el deber de información, de modo que «los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida». Con relación a los representantes legales de los trabajadores, si la cámara se quiere utilizar como herramienta de control de los trabajadores, se aplicaría el artículo 64.5.f) ET, de modo que tienen derecho a emitir informe con carácter previo. El deber de información es más amplio que el general dirigido a los clientes, ya que el trabajador debe saber no sólo lo explicitado en el artículo 22.4 LOPDyGDD sino también que la instalación de la cámara tiene como finalidad el control laboral. Este deber de información, sin embargo, se atenúa «en el supuesto de que se haya captado la

[16] RODRÍGUEZ ESCANCIANO, S. y ÁLVAREZ CUESTA, H., «La toma de decisiones automatizadas en el marco de la relación laboral: otra vuelta de tuerca al poder de dirección y vigilancia empresarial», *op. cit.*, p. 130.

comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos» en cuyo caso «se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica». Puede afirmarse, pues, que existen dos tipos de cámaras: las cámaras «informadas» (primer párrafo del artículo 89.1) y las «cámaras identificadas y no informadas» (segundo párrafo del artículo 89.1)[17]. Bajo la vigencia de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —en adelante, LOPD— la STC 39/2016 de 3 de julio había admitido este último tipo de cámara, aunque consideró que persistía »el deber de información del art. 5 LOPD», añadiendo que «sin perjuicio de las eventuales sanciones legales que pudieran derivar», para que el incumplimiento de este deber por parte del empresario implique una vulneración del artículo 18.4 CE debía valorarse la observancia o no del principio de proporcionalidad. Es decir, el Tribunal Constitucional situaba en dos planos distintos el deber de información derivado de la normativa de protección de datos y la posible ilegitimidad de la prueba obtenida por haberse producido una vulneración de derechos fundamentales, de modo que el incumplimiento de aquél no hacía que ésta fuera necesariamente ilícita. En opinión de Rojo Torrecilla, los redactores de la sentencia debían de estar pensando en la aplicación de la normativa sancionadora en el ámbito laboral, es decir la LISOS[18]. Varias sentencias del Tribunal Supremo mantuvieron esta doctrina relativizadora de la importancia del deber de información. Así, La STS de 1 de febrero de 2017 (rec. 3262/2015) en un caso donde la trabajadora fue objeto de un despido disciplinario por haber manipulado los tickets y hurtado diferentes cantidades, admitió como prueba la grabación de la cámara que había sido informada únicamente mediante el distintivo del artículo 22. Considera, no obstante, que frente a los defectos informativos que alegaron los demandantes pudieron reclamar a la empresa más información o denunciarla ante la AEPD, para que la sancionara por las infracciones que hubiese podido cometer[19]. En la STS de 21 de julio de 2021 (rec. 4877/2016)[20], se dio un paso más. La sala cuarta avaló la prueba suministrada por la parte empresarial, consistente en la grabación de una cámara «identificada pero no informada» en un supuesto donde los que se analizaba era un control puramente laboral, de condición de trabajo ordinaria, no de un hurto, ya que el trabajador que era vigilante de seguridad de un aeropuerto fue despedido por rellenar partes indicando que había realizado determinados controles, cuando

---

[17] Utilizamos las expresiones acuñadas por LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., «Control empresarial del uso de dispositivos digitales en el ámbito laboral, desde la perspectiva del derecho a la protección de datos y a la intimidad», *Revista Lex Social,* 2020, vol. 10, núm. 2, https://doi.org/ 10.46661/lexsocial.5075, p. 526.

[18] ROJO TORRECILLA, E., «Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (II)», *Blog El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas relaciones laborales*, entrada del 21 de marzo de 2016. Disponible en: http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de_21.html

[19] La misma reflexión en un caso idéntico encontramos en la STS de 31 de enero de 2017 (rec. 3331/2015) aplicada por la STSJ CV de 20 de abril de 2023 (rec. 3977/2022). También STS de 30 de marzo de 2022 (rec. 1288/2020).

[20] El mismo caso en STS de 25 de enero de 2022 (rec. 4468/2018).

no era cierto[21]. El Tribunal Supremo sentencia que su examen se ha de ceñir a si la prueba debió o no admitirse, sin que debiera extenderse a si se cumplieron todos los requerimientos de la legislación de protección de datos, algo que no impide que la empresa pueda ser responsable en el ámbito de la legislación de protección de datos. Incluso se invita al demandante a interponer una denuncia ante la AEPD. Todo ello en un caso en el que, como explica Duque González[22], se asume por parte de la Sala que no se ha cumplido la Ley orgánica de protección de datos, ni en el marco laboral entre empresa-trabajador, ni en el marco del tratamiento y cesión de datos ya que una empresa (el aeropuerto) suministró datos personales de terceros a otra (la empresa de seguridad) sin su consentimiento, sin información de ningún tipo y con el objeto de represaliar laboralmente a los mismos. Ya bajo la vigencia de la LOPDyGDD, en la STC 119/2022, de 29 de septiembre de 2022 se mantiene la misma doctrina, llegando a afirmarse que «el incumplimiento del deber de información afectaría, en esencia, al derecho a la protección de datos de carácter personal, no a la intimidad» (FJ 6). Con esta doctrina interpretativa se ha ahonda en la separación entre el derecho a la intimidad y el derecho de protección de datos. Para Duque González «todo lo expuesto tiene una lectura evidente para la Inspección de Trabajo y Seguridad Social, y es que los criterios, trámites y procedimientos establecidos por la AEPD para determinar la licitud de los tratamientos y las grabaciones que habitualmente se manejan en las actuaciones inspectoras, pueden no ser ni útiles ni necesarios»[23].

Pero cabría añadir una tercera modalidad de cámara para supuestos muy excepcionales admitidos por la STEDH (Gran Sala) de 17 de octubre de 2022 —Caso López Ripalda II—: las cámaras «ocultas» donde ni siquiera es exigible la información a través del dispositivo del artículo 22.4, cuando existan sospechas razonables de que se han cometido graves irregularidades. Es especialmente significativo que dicha sentencia del TEDH examinara el argumento de que la legislación española (la anterior LOPD) ya imponía por entonces la previa advertencia o información al trabajador sobre la videovigilancia, a pesar de lo cual el TEDH considera que la medida estaba justificada por la sospecha legítima de graves irregularidades y pérdidas y porque ninguna otra medida habría permitido alcanzar el objetivo legítimo. La legalidad de las cámaras ocultas ha sido confirmada tras la aprobación de la LOPDyGDD por la STS de 22 de julio de 2022 (rec. 701/2021). Tras recordar los pronunciamientos de la STEDH López Ripalda II, insiste la Sala especialmente en que en el caso objeto de la litis «se trata de

[21] Aplica esta doctrina la STSJ Comunidad Valenciana de 3 de noviembre de 2022 (rec. 1754/2022).
[22] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*
[23] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.* Sobre los criterios de la AEPD, *vid.* la Guía de la AEPD «La protección de datos en las relaciones laborales» (mayo de 2021), disponible en: https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf (última consulta 26 de octubre de 2022).

examinar la validez probatoria de la videovigilancia efectuada en un juicio por despido, a la vista de la carga de la prueba que corresponde al empresario y la consiguiente necesidad de poder aportar medios pertinentes de prueba, y no de otras consecuencias que la conducta empresarial puede tener desde la perspectiva más amplia de la legislación de protección de datos en su conjunto. En efecto, una cosa es que, en un supuesto de las singulares características como el que estamos examinando, la ausencia de información no deba obligadamente conducir a la nulidad de la prueba de videovigilancia, necesaria para acreditar el incumplimiento y su autoría, y, otra, que la empresa no pueda ser declarada responsable de un posible incumplimiento de la legislación de protección de datos con las posibles consecuencias administrativas o civiles, o de otra naturaleza, que ello pueda conllevar.»

Continúa diciendo el artículo 89.2 que «en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos». La instalación de cámaras en dichos sitios afectaría gravemente al derecho a la intimidad[24]. Por su parte, el apartado 3 analiza la utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo (audiovigilancia). Se admitirá «únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley».

Tanto en la videovigilancia como en la audiovigilancia se ve afectado el derecho a la protección de datos, ya que el propio legislador indica que se van a «tratar» las «imágenes» y los «sonidos» que serán datos personales en la medida en que permitan identificar a las personas grabadas. Por otro lado, en el artículo 89 hay una remisión expresa al artículo 22 LOPDyGDD en relación con el contenido que debe tener el contenido de la información[25]. Pero también puede producirse una intromisión de especial gravedad en la intimidad, principalmente cuando las cámaras se instalan en lugar de descanso y ocio y cuando la grabación incluye la voz[26]. En este sentido es muy fre-

---

[24] Respecto de la instalación de cámaras en lugares de descanso o esparcimiento de trabajadores, señala la STSJ Canarias/Las Palmas de Gran Canaria, de 15 de noviembre de 2022 (rec. 1265/2022) que «la correcta interpretación que debe darse al art. 89. 2 de la LOPD es que la prohibición con la que se inicia la literalidad del precepto no es petrificada, absoluta e incondicional y puede ceder en aquellos casos en los que se supere el test de constitucionalidad referido, lo que exigirá un análisis de ponderación caso a caso. Lo contrario nos podría llevar a situaciones absurdas, en términos de justicia material».

[25] GARCÍA RUBIO, A., «Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa», *op. cit.*, p. 34.

[26] En el PS/00178/2022 la AEPD sanciona a la empresa por comisión de infracción muy grave ya que realizó tratamientos de datos sin disponer de base legítima, vulnerando lo establecido en el artículo 6 del RGPD, por lo que

cuente que se aleguen ambos derechos frente a las prácticas empresariales de videovigilancia[27] y audiovigilancia aunque, dado que se trata de derechos autónomos, no faltan sentencias donde el demandante invoca sólo uno de ellos, por ejemplo, en videovigilancia sólo el derecho de protección de datos[28].

2.3. El derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

En el artículo 90 se regula el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 ET y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. A diferencia de los supuestos anteriores, donde no se menciona, pero está igualmente incluido, se indica que «igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión»[29]. De nuevo tenemos que decir que el derecho a la protección de datos parece ser el principal bien jurídico protegido. En primer lugar, el artículo 4 RGPD cuando define el dato personal se refiere expresamente a los datos de localización[30]. Por otro lado, la regulación del derecho no sólo pivota en torno al deber de información, que forma parte del contenido esencial del derecho de protección de datos, sino que además se remite a la obligación de cumplir con los derechos ARCO[31]. La información exigida es nuevamente la completa, la que impone la normativa de protección de datos, a la que debe añadirse la información relativa a la posibilidad de utilizar el sistema de geolocalización para controlar la actividad

---

podrían suponer la comisión de una infracción tipificada en el artículo 83.5 del RGPD. Ello es así, porque se entiende desproporcionada la captación de la voz tanto de los trabajadores como de clientes de la parte reclamada para la función de videovigilancia pretendida, para el control del cumplimiento por los trabajadores de sus obligaciones y deberes laborales. Se tiene en cuenta que la grabación de voz supone una mayor intromisión en la intimidad.

[27] Por ejemplo, en la STEDH de 9 de enero de 2018 (López Ripalda I) la demanda por videovigilancia irregular tomó como fundamento el derecho al respeto de la vida privada, ex art. 8 CEDH, aunque en su fundamentación jurídica el TEDH tomará como referencia los apartados 1 y 4 del art. 18 CE y la normativa sobre protección de datos.

[28] Por ejemplo, STS de 30 de marzo de 2022 (rec. 1288/2020) y STSJ de 9 de febrero de 2023 (rec. 221/2022).

[29] RODRÍGUEZ ESCANCIANO S. y ÁLVAREZ CUESTA, H., «La toma de decisiones automatizadas en el marco de la relación laboral: otra vuelta de tuerca al poder de dirección y vigilancia empresarial», *op. cit.*, p. 135.

[30] GONZÁLEZ RODRÍGUEZ, R., «Los derechos fundamentales como límite difuso al control tecnológico en el ámbito laboral: luces y sombras de la primera regulación específica sobre la materia», *Revista de Trabajo y Seguridad Social, op. cit.*, p. 88.

[31] Por ejemplo, STS de 15 de septiembre de 2020 (rec. 528/2018).

laboral y, en su caso, para adoptar medidas disciplinarias[32]. Sin embargo, la vulneración del derecho a la intimidad no es siempre clara en este último método. Por ejemplo, en la colocación de un sistema de geolocalización en un vehículo móvil, que lo que hace es registrar cuando arranca y se detiene el vehículo y dónde se encuentra físicamente, puede no revelar datos de la vida privada, si el sistema no permite captar circunstancia alguna de sus ocupantes[33]. El deber de información se hace extensivo a los representantes de los trabajadores que aparecen esta vez como meros receptores.

2.4. El derecho a la desconexión digital en el ámbito laboral

Finalizamos el estudio de los derechos digitales con el artículo 88 que regula el derecho a la desconexión digital en el ámbito laboral. Los trabajadores y los empleados públicos «tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar». Las modalidades de ejercicio de este derecho «atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores». El empleador, «previa audiencia de los representantes de los trabajadores,» debe elaborar «una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática». Se debe preservar en particular «el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas». Con escasas alteraciones la norma se ha volcado en el artículo 17 LTD que añade que «Los convenios o acuerdos colectivos de trabajo podrán establecer los medios y medidas adecuadas para garantizar el ejercicio efectivo del derecho a la desconexión en el trabajo a distancia y la organización adecuada de la jornada de forma que sea compatible con la garantía de tiempos de descanso». La SAN de 22 de marzo de 2022 (rec. 33/2022) ha interpretado el artículo 88 en el sentido de que los límites al derecho de desconexión digital no los puede establecer unilateralmente el empresario sino que como indica el propio precepto «se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores»[34].

---

[32] GARCÍA RUBIO, A., «Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa», *op. cit.*, p. 31.

[33] STS de 15 de septiembre de 2020 (rec. 528/2018), SJSO núm. 2 Palencia, de 15 de marzo de 2023 (rec. 560/2022).

[34] La sentencia habla de los límites a la desconexión digital en el teletrabajo, pero basa su respuesta directamente en el artículo 88 LOPDyGDD por lo que esta interpretación es extrapolable al trabajo presencial.

Por lo que se refiere a los bienes jurídicos protegidos, se trata de un «derecho multiforme que involucra a distintos y diversos derechos a los que se dirige y pretende proteger». Por un lado, se protegen derechos relacionados con el tiempo de trabajo, a saber, el derecho al descanso, los permisos y las vacaciones; por otro, también se dirige a proteger el derecho a la intimidad personal y familiar, así como el derecho a la conciliación de la vida laboral, personal y familiar; y, por último, el derecho a la seguridad y salud en el trabajo, con el objetivo de evitar riesgos psicosociales, refiriéndose expresamente la ley a la fatiga informática[35]. Al menos como regla general, no se ha concebido como un derecho que afecte específicamente al derecho a la intimidad[36], lo que no impide que en atención a las circunstancias del caso concreto sí se pueda ver afectado. De hecho, en el Criterio Técnico 104/2021, sobre actuaciones de la Inspección de Trabajo y Seguridad Social en riesgos psicosociales (14 de abril de 2021) se indica que en situaciones de estrés motivadas por no respetarse el derecho a la desconexión digital se puede producir una vulneración más específica del derecho a la intimidad. Pensemos, por ejemplo, en la obligación de conectarse telemáticamente con la empresa fuera de horas de trabajo a través de cámaras que revelen datos íntimos del trabajador y de su familia (ej: creencias religiosas o políticas, determinadas circunstancias familiares, etc.)[37]. Pero su objetivo tampoco es proteger el derecho a la protección de datos[38], de modo que han sido más bien razones de oportunidad las que han llevado al legislador a incluirlo en esta ley, creando con ello confusión.

3. PROCEDIMIENTO SANCIONADOR

Entre las «normas de orden social» por cuyo cumplimiento vela la ITSS nos interesa destacar principalmente los siguientes artículos del ET: 1. el artículo 4.2.e) ET que recoge el derecho del trabajador «al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo». 2. el artículo 20 bis ET que, a nuestro jui-

---

[35] MORENO SOLANA, A., «La desconexión digital en el teletrabajo como medida de prevención de los riesgos psicosociales», *Anuario iet de trabajo y relaciones laborales,* vol. 8, 2022, p. 123 (https://doi.org/10.5565/rev/aiet.109).

[36] La STSJ Cataluña de 5 de mayo de 2023 (rec. 704/2022) declaró extinguido el contrato porque el empleado estaba sometido a una carga de trabajo desmesurada, con jornadas muy prolongadas y horarios intempestivos, vulnerando el derecho al descanso y a la desconexión digital. Como consecuencia de ello, tuvo una patología psiquiátrica que le mantuvo en IT durante un largo periodo. Sin embargo, no procede una indemnización adicional de 120.000 € porque el derecho a la desconexión digital no está recogido en nuestra Constitución como un derecho fundamental (aunque sí para el Derecho de la Unión). Está mencionado en el art. 40.2 CE que recoge los principios rectores de la política social y económica. Además, no manifestó en ningún momento sus dificultades en el trabajo y la patología fue tratada como enfermedad común no impugnada. Inexistencia de acoso laboral.

[37] ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías *de lege data», op. cit*., p. 70.

[38] ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías *de lege data», op. cit*., p. 70.

cio, debe ponerse en conexión con el artículo 4.2.e) ya que tiene por finalidad reforzar la garantía del derecho a la intimidad de los trabajadores cuando la empresa lleva a cabo un control por medios tecnológicos. En ocasiones, la intensidad del control laboral puede dar lugar a conductas de acoso[39]. 3. en el ámbito del trabajo a distancia hay que tener en cuenta los arts. 17 (derecho a la intimidad y a la protección de datos) y 18 (derecho a la desconexión digital) de la LTD. 4. en relación con el derecho a la desconexión digital pueden resultar también afectadas las normas relativas al tiempo de trabajo (artículos 34 a 38 ET) y la normativa de prevención de riesgos laborales.

En la LISOS hay varios tipos infractores en los que podría encontrar acomodo el incumplimiento de estos preceptos:

1. el artículo 8.11 tipifica como falta muy grave «los actos del empresario que fueren contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores». Como explica, Duque González[40] «el concepto de dignidad del trabajador hace que todos estos preceptos, y la tutela intrínseca a los mismos por parte de la ITSS, no se circunscriban únicamente al derecho a la intimidad, sino a la totalidad de los derechos fundamentales de los trabajadores que deban ser respetados en la relación de trabajo, en tanto en cuanto sustento de la dignidad personal de aquellos»[41]. Se incluiría también, por tanto, el derecho al secreto de las comunicaciones, que puede ser vulnerado en un caso de control de correo electrónico del trabajador, de fiscalización de sus redes sociales privadas o de conversaciones de WhatsApp de los empleados. No sería competente, sin embargo, para sancionar por vulneración del derecho de protección de datos del trabajador ya que su competencia está reservada a la AEPD[42], autoridad estatal de control independiente que, como regla general, actúa en los casos en los que haya un tratamiento de datos, es decir «es necesario que se recaben datos para incorporarlos a un fichero, de tal manera que, con base en ellos se pueda decir que hay un *tratamiento*»[43]. La LOPDyGDD dedica el Título IX al procedimiento sancionador.

---

[39] En 2020 fue noticia que «La Inspección de Trabajo insta a Prosegur a que deje de llamar y mandar correos a sus empleados fuera del horario laboral La práctica vulnera la desconexión digital y el derecho a la intimidad de sus trabajadores, según la Inspección, que exige a Prosegur que ciña su comunicación a la jornada de trabajo». En concreto la ITSS advierte a la empresa de que cese en su conducta con apercibimiento de que en caso de no hacerlo será sancionado por acoso con base en el artículo 8.13 LISOS. Fuente: elDiario.es, noticia del 6 de octubre de 2020, https://www.eldiario.es/economia/inspeccion-trabajo-insta-prosegur-deje-llamar-mandar-correos-empleados-fuera-horario-laboral_1_6272926.html (última consulta 20 de octubre de 2022).

[40] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*

[41] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*

[42] La AEPD es un supuesto inédito de organismo sancionador de un único derecho fundamental, el recogido en el artículo 18.4 CE. DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*

[43] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*

2. Si se han incumplido los distintos deberes de información y consulta con los representantes legales de los trabajadores, presentes en los artículos 87 a 90, hay que tener en cuenta que el artículo 7.7 LISOS que tipifica como infracción grave «La transgresión de los derechos de información, audiencia y consulta de los representantes de los trabajadores y de los delegados sindicales, en los términos en que legal o convencionalmente estuvieren establecidos», lo que tiene gran importancia de cara a los protocolos que exige la LOPDyGDD[44].

3. En relación con el derecho a desconexión digital, se plantea un problema inicial porque los artículos 20 bis) ET y 88 LOPDyGDD parecen configurarlo como un derecho, no como un deber empresarial. Es más correcta la redacción del artículo 18 LTD que habla claramente del «deber empresarial de garantizar la desconexión». Las dudas que podían existir respecto a la ubicación en los tipos infractores en la LISOS han sido resueltas por el Criterio Técnico 104/2021[45]. De esta forma, se aplicarían las infracciones tipificadas en los arts. 7, 8 y 12 LISOS en los siguientes términos:

- La violación de los límites legales de jornada de los arts. 34 a 36 ET, entrarían siempre en la infracción grave del artículo 7.5 LISOS por «la transgresión de las normas y los límites legales o pactados en materia de jornada, trabajo nocturno, horas extraordinarias, horas complementarias, descansos, vacaciones, permisos, registro de jornada y, en general, el tiempo de trabajo a que se refieren los artículos 12, 23 y 34 a 38 del Estatuto de los Trabajadores». Es preciso aclarar, sin embargo, que la sanción no opera por el mero hecho de enviar los correos electrónicos, sino que es preciso que la empresa no haya dejado claro que no existe obligación de contestar correos fuera de las horas de trabajo. Si no lo ha hecho, se produciría una ampliación encubierta de la jornada[46]. Esta cuestión debe aparecer explicitada en el Protocolo de desconexión digital.

- La omisión de las medidas de protección y garantía del derecho a la intimidad y desconexión del artículo 88 LOPDyGDD, en particular la falta de una política interna dirigida a trabajadores, incluida los que ocupen puestos directivos, en la que definirán los modelos de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática, como ocurre en el teletrabajo, estaría tipificada dentro del artículo 7.10 LISOS por

---

[44] AYERRA DUESCA, N. J., «El derecho a la desconexión digital desde un punto de vista de la prevención de riesgos laborales», *op. cit.*, p. 55.

[45] El criterio pretende adaptar el contenido de la Guía y los Principios del Comité de Altos Responsables de la Inspección de Trabajo (en adelante, «SLIC») al marco legal vigente en España.

[46] Hay que tener en cuenta que puede ser habitual recibir correos fuera de la jornada particular del trabajador, en empresas con horarios flexibles con distintas horas de entrada, salida y de comida, empleados en países con distinto huso horario, reducciones de jornada, empleados y/o jefes de viaje en el extranjero en países con diferencia horaria…).

«actos u omisiones que fueren contrarios a los derechos de los trabajadores reconocidos en el artículo 4 de la Ley del Estatuto de los Trabajadores, salvo que proceda su calificación como muy graves, de acuerdo con el artículo siguiente».

- La constatación de una efectiva violación o atentado al derecho a la intimidad constituiría una infracción muy grave de acuerdo con los previsto en el artículo 4.2.e) ET y 8.11 LISOS. Esto ocurriría en caso de que se concretara en algún trabajador el riesgo psicosocial como podría ser Burnout o tecnoestrés. También un envío masivo o continuo podría entenderse como una coacción al trabajador para responder y contraria a la dignidad del trabajador[47].

- En cualquier caso, señala el criterio, serían de aplicación las normas relativas a la prevención de riesgos laborales (que también concurren en estos supuestos) cuando sea procedente la emisión de un requerimiento de medidas preventivas[48] y, en su caso, la extensión de acta de infracción o la imposición del recargo de prestaciones de Seguridad Social. Para ello es preciso admitir que el artículo 88 LOPDyGDD es «una verdadera norma en materia de prevención de riesgos laborales «aunque no se encuentre inserta en dicho cuerpo normativo»[49]. De esta manera se salva el escollo planteado por la LISOS cuando en la mayoría sus preceptos hace referencia expresa a obligaciones fijadas «en la normativa de prevención de riesgos laborales» o «con el alcance y contenido establecidos en la normativa de prevención de riesgos laborales». Hay varios preceptos de la LISOS que serían aplicables. Así, las infracciones leves de los artículos 11.4 y 11.5. En ellos se subsumirían los supuestos de incumplimiento derivados de la falta de elaboración de una política interna que defina las modalidades de ejercicio de la desconexión digital[50]. También se aplicarían los artículos 12.1, 12.4, 12.6 12.8, 12.11 y 12.12 relacionados con incumplimientos de derivados de la obligación de integrar la prevención de riesgos laborales «a través de la implantación del plan de prevención y su aplicación a través de la evaluación de riesgos

---

[47] Recientemente ha sido noticia que la Inspección de Trabajo de Tarragona en una actuación frente a una empresa de seguridad, ha calificado como muy graves los hechos ya que los empleados no sólo recibían llamadas y correos electrónicos de sus superiores fuera de su horario laboral, sino que respondían a la mayor brevedad por temor a posibles represalias y al impacto negativo que no hacerlo pudiera tener en el sistema de incentivos de la compañía. Fuente: law21, disponible en https://law21.xyz/el-derecho-a-la-desconexion-digital-interpretado-por-la-inspeccion-de-trabajo/ (última consulta 12 de octubre de 2023).

[48] Por ejemplo, la ITSS ha requerido a EULEN a que elabore el plan de desconexión digital después de que alternativa sindical denunciara que la mercantil no tiene elaborado el plan de desconexión digital y que perturba el descanso de los vigilantes mediante email o WhatsApp para cubrir descubiertos. Noticia y acta disponible en: https://alternativasindical.es/inspeccion-de-trabajo-extiende-diligencia-de-cumplimiento-del-plan-de-desconexion-digital-contra-eulen-a-denuncia-de-alternativasindical/ (última consulta 6 de octubre de 2023).

[49] ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías *de lege data», op. cit.*, p. 86.

[50] AYERRA DUESCA, N. J., «El derecho a la desconexión digital desde un punto de vista de la prevención de riesgos laborales», *op. cit.*, p. 55.

–con sus correspondientes revisiones, actualizaciones, controles y registro de los datos obtenidos— y de la planificación de la actividad preventiva»[51].

4. LA POSIBLE CONCURRENCIA DE COMPETENCIAS ENTRE LA INSPECCIÓN DE TRABAJO Y LA AEPD

Retomando la pregunta relativa a la posible concurrencia de competencias entre la ITSS y la AEPD para sancionar actos contrarios a las garantías de los derechos digitales, hay que decir que bajo la vigencia de la anterior LOPD fueron mucho los expedientes tramitados por dicha autoridad relativos tanto a vigilancia de correos electrónicos de trabajadores[52], como a videovigilancia[53]. Tras la aprobación de la nueva ley, el problema es que los límites entre los derechos digitales laborales y las obligaciones de protección de datos son muy difusos. Hemos visto a lo largo de este estudio que, con la excepción del derecho a la desconexión digital, se produce una afectación de mayor o menor intensidad tanto del derecho a la protección de datos como del derecho a la intimidad. El problema es que el deber de información forma parte del contenido esencial del derecho a la protección de datos, pero también en el ámbito del derecho a la intimidad se hace depender de la información previa proporcionada al trabajador, la existencia de la expectativa de intimidad. En este sentido, cuando no se respeta el deber de información se vulneran ambos derechos fundamentales, si bien, el contenido del deber de información es más amplio en el caso de la videovigilancia y la geolocalización, aunque algunos autores aplican el artículo 5 RGPD (principios relativos al tratamiento) también a la vigilancia de los dispositivos digitales[54]. Estas reflexiones, sin embargo, parece que deben matizarse como consecuencia de la doctrina judicial que tiende a relativizar la importancia del deber de información en el derecho a la intimidad, de modo que sería posible incurrir en un incumplimiento de la normativa de protección de datos, sin que se considerase contraria al derecho a la intimidad la prueba obtenida.

El legislador no ha introducido ni en la LOPDyGDD ni en la LISOS ningún precepto que regule la posible concurrencia entre las sanciones de la AEPD y las de la ITSS. El

---

[51] AYERRA DUESCA, N. J., «El derecho a la desconexión digital desde un punto de vista de la prevención de riesgos laborales», *op. cit.*, p. 55. ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías *de lege data», op. cit.,* pp. 85-86.

[52] Aunque referida a funcionario público interesa la SAN (Sala de lo contencioso) de 10 de junio de 2022 (rec. 1684/2020) que conoció del recurso contencioso-administrativo contra la Resolución de la Directora de la AEPD de fecha 27 de noviembre de 2020 (PS/00062/2019) que declaró que el Ayuntamiento había cometido infracción del artículo 6 de la LOPD por el registro del ordenador del funcionario, sin haber sido informado previamente. Tras aplicar la doctrina Barbulescu, considera vulnerado el artículo 6 LOPD. No obstante, al ATS de 19 de enero de 2023 (rec. 6949/2022) ha declarado que la cuestión planteada (la aplicación de la doctrina Barbulescu al ámbito de la función pública) tiene contenido casacional y ha admitido el recurso de casación contra la sentencia.

[53] PS/00112/2015 se sancionó a la empresa.

[54] GOÑI SEIN, J. L., «Uso de los dispositivos digitales en el ámbito laboral», op. cit., pp. 27-29.

artículo 47 LOPDyGDD precisa que «corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo». Dicha norma podría interpretarse en el sentido de que «la AEPD tiene competencias para supervisar la aplicación de la completa normativa establecida en la LOPD»[55], incluidos los derechos digitales laborales. Sin embargo, dicha interpretación no es del todo correcta. En primer lugar, como ha señalado la doctrina, la LOPDyGDD no es la norma adecuada para para regular las infracciones y sanciones en el orden social, sino que un adecuado régimen disciplinario para sancionar al «empresario infractor» debería haber venido de la mano de la modificación de la LISOS[56]. En segundo lugar, aunque esta interpretación fuera cierta, la competencia de la AEPD respecto de los derechos digitales no sería completa sino que seguiría limitada a los aspectos relacionados exclusivamente con la protección de datos. En este sentido, resulta muy significativo que el Título X no sólo se sitúe después del bloque normativo regulador de la protección de datos, incluyendo la AEPD y el régimen sancionador. La consecuencia que extrae Duque González es que la fiscalización de los derechos digitales de los trabajadores establecidos en la LOPDy GDD «corresponde al organismo especializado en el ámbito laboral, esto es, a la ITSS» quien, por otro lado, tiene en cuenta los criterios y directrices emitidos por la AEPD para valorar la vulneración o no del derecho fundamental de los trabajadores a su intimidad y dignidad en la relación de trabajo[57]. De hecho, en la ley orgánica la sanción se impone al empresario, no por su condición de empleador, sino por su condición de responsable o encargado del tratamiento de datos. Sin embargo, hay que tener en cuenta que el artículo 2.1 LOPDyGDD dispone que «Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.» Es llamativo que el legislador incluya los artículos 89 y 90 pero excluya los artículos 87 y 88 LOPDyGDD. Según ello, dentro de los tres derechos a la intimidad regulados en la LOPDyGDD los relativos a videovigilancia y geolocalización podrían tener un régimen diferente por su estrecha conexión con el derecho a la protección de datos y el RGPD, ya que suponen un tratamiento de datos. Esta postura ha sido la que ha seguido la AEPD en el procedimiento E/10250/2019 –Resolución de 3 de junio de 2019– confirmado, tras interponer el trabajador recurso de reposición, por resolución

---

[55] MERCADER UGUINA, J., «El control sobre el uso de los dispositivos digitales y sobre el Derecho a la Desconexión en la empresa no es competencia de la AEPD», *op. cit.*

[56] ALTÉS TÁRREGA, J. A. y YAGÜE BLANCO, S., «A vueltas con la desconexión digital: eficacia y garantías de *lege data», op. cit.*, p. 84. Explica el autor, en relación con el derecho a la desconexión digital que hubo propuestas por parte de la doctrina de inclusión de infracciones normativas bien en la subsección 1.ª del capítulo II (infracciones en materia de relaciones laborales individuales y colectivas) o en la sección 2.ª del mismo capítulo (infracciones en materia de prevención de riesgos laborales), aunque ninguna de ellas fue acogida por el legislador.

[57] DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit.*

RR/00312/2020-, donde se resuelve el archivo de actuaciones frente a una reclamación formulada por un empleado que denuncia a su empresa empleadora ante el acceso de ésta a su correo electrónico corporativo sin que se le hubiera informado de los criterios de utilización o política de uso de los medios informáticos, lo que, a juicio del trabajador, vulneraba su derecho a la protección de datos personales[58]. Aunque la AEPD entiende cumplido con el deber de advertencia a que se refiere el artículo 87 LOPD, la Agencia utiliza esta resolución para hacer algunas precisiones importantes sobre las dudas existentes sobre su competencia. En primer lugar, precisa que «el preámbulo de la LOPD señala que la ley en su Título X acomete la tarea de reconocer una serie de derechos digitales de los ciudadanos conforme el mandato establecido en la Constitución y, entre ellos, el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral. Estos derechos no se encuentran regulados en el RGPD y han sido incorporados en la nueva LOPD». Añade que en «el artículo 1 de la citada Ley se señala que esta tiene por objeto, en primer lugar, adaptar el ordenamiento jurídico español al RGPD en lo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y completar sus disposiciones y, en segundo lugar, garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución». En cuanto a su ámbito de aplicación viene regulado en su artículo 2, y en su apartado 1, dicho ámbito se encuentra vinculado en relación con cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Sin embargo, «en cuanto a los preceptos digitales se trata de declaraciones de derechos sobre los que no se regulan ni se establecen mecanismos que los garanticen, es decir, ni se señala, ni en ningún caso se establece, que la AEPD tenga competencias para garantizar estos derechos quedando fuera de sus atribuciones, como a sensu contrario, si se establece tanto en el RGPD como en la LOPD en relación a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Por consiguiente, de conformidad con el artículo 2.1 de la LOPD de los citados artículos tan solo del 89 a 94 si son competencia de la propia AEPD a nivel de garantizar su cumplimiento y ejercicio»[59]. Al respecto son numerosas las resoluciones de dicha autoridad indepen-

[58] Explica Mercader Uguina que, antes de que recayera esta resolución, en diversas intervenciones públicas representantes de la AEPD habían venido afirmando verbalmente la exclusión de su ámbito de competencias de lo dispuesto en los artículos 87 y 88 LOPD. MERCADER UGUINA, J., «El control sobre el uso de los dispositivos digitales y sobre el Derecho a la Desconexión en la empresa no es competencia de la AEPD», *op. cit.*

[59] *Vid*. también MERCADER UGUINA, J., «El control sobre el uso de los dispositivos digitales y sobre el Derecho a la Desconexión en la empresa no es competencia de la AEPD», *op. cit.* Sin embargo, ha sido noticia recientemente que «La AEPD intensifica la vigilancia por el incumplimiento de la Desconexión Digital» (noticia del 2 de octubre de 2023). En este contexto, la AEPD está investigando a Securitas Seguridad España, S. A., en su Delegación de Cádiz, por incumplir con este derecho, utilizando WhatsApp para enviar información operativa, personal y sindical a sus trabajadores fuera del horario laboral. Se ha informado al denunciado de la posible infracción de los arts. 32, 5.1.b), 5.1.f) y 6.1 del RGPD y de la necesidad de adecuar los tratamientos que realiza a lo dispuesto en la citada normativa. Por último, la AEPD recuerda que de constatarse la no adopción por parte del denunciado

diente recaídas en relación con videovigilancia[60] y geolocalización[61], tras la entrada en vigor del RGPD y de la ley orgánica, donde se sanciona a la empresa (o se apercibe a la Administración empleadora) por falta de información previa a los trabajadores o por utilizarse los dispositivos digitales de control para una finalidad distinta a la comunicada a la Agencia. En algunas de ellas consta que los trabajadores habían presentado previamente denuncia ante la Inspección de Trabajo cuyo informe se adjunta al procedimiento[62]. Tienen en común que se aprecia violación de varios artículos del RGPD: 5.1.b) y f) —principios relativos al tratamiento—, 6 —licitud del tratamiento— y 13 —información que deberá proporcionarse cuando los datos se obtengan del interesado—. En la misma línea puede verse la Resolución de la AEPD de 22 de enero de 2021 (E/00377/2020) y también el informe de la ITSS de 9 de mayo de 2023 en contestación a denuncia presentada por Alternativa Sindical, donde recuerda que la AEPD tiene competencia exclusiva sobre las reclamaciones formuladas por las personas afectadas frente a los responsables del tratamiento de datos en materia de videovigilancia, sin embargo, concluye lo mismo con el derecho a la desconexión digital.

La separación entre los artículos 87 y 88 que serían competencia preferente de la ITSS y los artículos 89 y 90 que serían competencia preferente de la AEPD, no es sin embargo tan sencilla. Por un lado, dentro del artículo 87 en la medida en que los datos recabados se incorporen a un fichero que sea objeto de tratamiento, será preciso cumplir la normativa de protección de datos[63]. Por otro lado, incluso en caso de videovigilancia y geolocalización, no sería necesario aplicar el principio non bis in ídem si la conducta objeto de fiscalización fuera más amplia que la mera grabación o videovigilancia, como en los casos de acoso, en donde la videovigilancia abusiva puede utilizarse como un medio más de hostigamiento. En este caso no habría coincidencia de hechos y se podría hablar de concurso real de infracciones pudiendo sancionarse por

---

de las medidas correctoras que, en su caso, fueran necesarias, podrían iniciarse las actuaciones previstas para supuestos de incumplimiento en la normativa precitada, acordes con las potestades de investigación y sancionadora de la Agencia. Noticia disponible en https://alternativasindical.es/la-agencia-espanola-de-proteccion-de-datos-advierte-a-securitas-por-incumplir-con-la-desconexion-digital/ (última consulta 6 de octubre de 2023).

[60] Existen varias resoluciones de la AEPD recaídas tras denuncias de los trabajadores motivadas por la falta de información o por la ubicación en zonas privadas. Por ejemplo, EXP20210247, PS/00337/2021, PS/00413/2020, PS/00337/2021, PS/00226/2021, PS/00506/2020, E/09001/2018, PS/00178/2022.

[61] *Vid.* PS/00124/2019 AEPD. La SAN (sala de lo contencioso) de 14 de junio de 2021 (rec. 1770/2019) conoció del recurso contra la resolución de la directora de la AEPD que desestimó el recurso de reposición contra la Resolución de 1 de abril de 2019 que acordó la inadmisión a trámite de la reclamación presentado por un trabajador por instalación de GPS en el coche para geolocalización que se hacía extensiva durante festivos y fines de semana, sin haber sido informado previamente. La resolución ya aplica el artículo 90.

[62] En el PS/00345/2020 se presenta denuncia de los trabajadores contra la comunidad de propietarios. Los trabajadores avisaban de que había sido interpuesta denuncia ante la ITSS. se denuncia la presencia de diversas cámaras «en espacios peatonales, zonas comunes (como piscinas y zonas de trabajo)».

[63] En el PS/00073/2019 sí se controló la validez del uso que realizaba el Ayuntamiento de Alcobendas de las grabaciones de las radiotransmisiones del Centro integral de comunicaciones (CICO) con fines disciplinarios de los policías locales. La AEPD reconduce el supuesto al art. 87 LOPDyGDD. Las actuaciones, sin embargo, se archivaron por apreciar la AEPD que no había existido tratamiento de datos.

separado cada una de ellas. También cuando las cámaras se instalan en zonas de descanso o esparcimiento de los trabajadores podría apreciarse que la vulneración del derecho a la intimidad es de tal gravedad que podría ser sancionada por la ITSS, con independencia de que la AEPD sancione por infracción de la normativa de protección de datos, ya que claramente los bienes jurídicos afectados son distintos (intimidad y protección de datos). También podría haber una coincidencia parcial reconducible a un concurso medial (es decir una infracción se cometió como medio de otra), en cuyo caso se debería imponer la sanción por la infracción más grave cometida, conforme al artículo 29.5 LRSP. En todo caso, si la ITSS inicia una investigación, tras la atenuación del deber de información que se aprecia respecto de las cámaras identificadas pero no informadas y de las ocultas[64] para determinar la concurrencia, o la exclusión del tipo, la ITSS deberá realizar un juicio de proporcionalidad que, partiendo de la existencia de un fin legítimo, valore la idoneidad, necesidad y proporcionalidad de la medida, y valorar el conocimiento que pueda tener el trabajador sobre el hecho de estar siendo grabado, sea cual sea la finalidad de la cámara, e incluso sea cual sea el titular de ésta. El resto de las cuestiones reguladas en la normativa de protección de datos parecen totalmente accesorias, sin perjuicio de la actuación de la AEPD, y sin perjuicio de que algunas de ellas, como los derechos de información, consulta y audiencia de los representantes de los trabajadores, como hemos visto anteriormente, sí estén tipificadas como infracciones administrativas en la LISOS, y sigan quedando en la esfera de actuación de la ITSS. En materia de prevención de riesgos laborales, «si la videovigilancia ilícita o abusiva generara, o pudiera generar, una situación de estrés dañina para la salud del empleado, las eventuales infracciones tampoco incurrirían necesariamente en *bis in ídem*, ni con las infracciones tipificadas en la LOPDyGDD, ni con las infracciones en materia laboral tipificadas en la LISOS, en tanto en cuanto se persiguen incumplimientos de las obligaciones establecidas en la LPRL, cuyo bien jurídico es diverso (proteger la salud del empleado). En este supuesto los hechos imputados podrían ser también divergentes, tales como una falta de evaluación de riesgos específica..., etc. Todo ello hace conveniente que la intervención de la ITSS deba prevalecer en estos casos sobre la de la AEPD, sin perjuicio de que se puedan establecer mecanismos de coordinación, colaboración y cooperación»[65]. Lo ideal sería que hubiera un procedimiento de coordinación entre la ITSS y la AEPD, mientras tanto, encontramos algunos supuestos donde ha existido una actuación de un organismo ante el otro, normalmente la ITSS ante la AEPD. Por ejemplo, en la STSJ Canarias/Las Palmas de 31 de mayo de 2021 (rec. 281/2021) se estimó la demanda sobre tutela de derechos fundamentales presentada por un trabajador por «vulneración del derecho fundamental

[64] DUQUE GONZÁLEZ M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit*.

[65] Las reflexiones sobre la aplicación de *non bis in idem* son de DUQUE GONZÁLEZ, M., «El procedimiento administrativo de la Agencia Española de Protección de Datos e incidencias con la actuación de la Inspección de Trabajo y Seguridad Social», *op. cit*.

del trabajador actor protegido en el art. 18 CE (derecho a la intimidad) en relación con las previsiones contenidas en el art. 89. 1 y 2 de la LOPD, este último apartado, que prohíbe expresamente la instalación de cámaras de vigilancia en lugares de descanso o esparcimiento». Fue la propia ITSS la que denunció ante la AEPD[66], aunque dicha autoridad por Resolución de 9 de enero de 2020 había comunicado a la empresa el archivo de actuaciones.

[66] Fuente: AEPD: https://legalforma.com/camara-sin-cartel-informativo-para-controlar-trabajadores